MATERIA CULTURA DIGITAL I
INFORMACIÓN SOBRE IDENTIDAD Y CREDENCIAL / LECTURA NO. 2

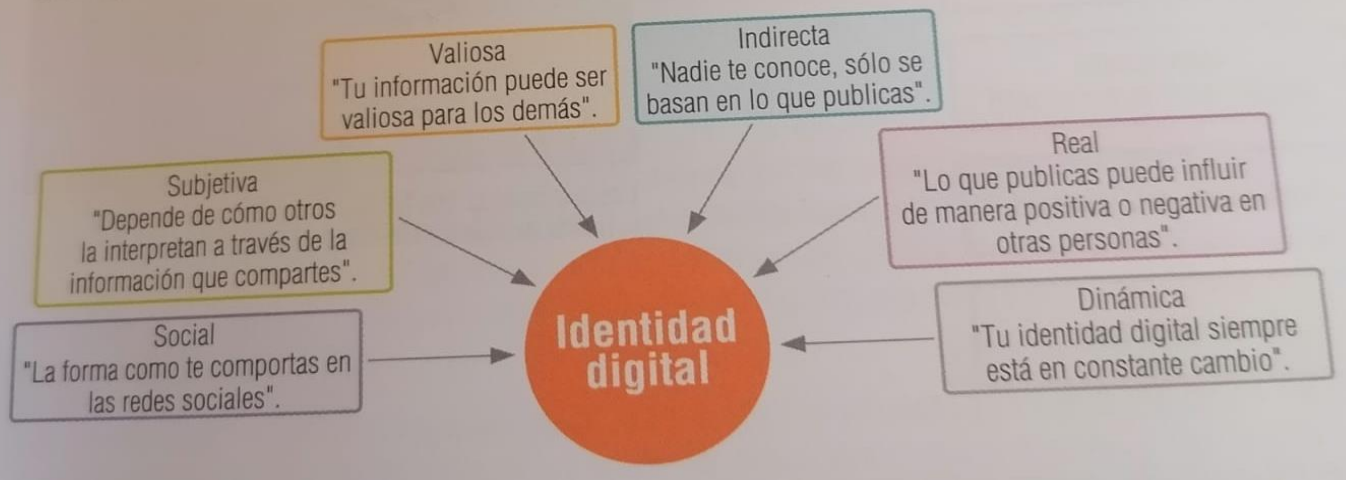
ACCIÓN

A medida que avanzamos en el siglo XXI, nos vemos más introducidos en un universo digital interconectado que representa la esencia misma de lo que significa ser humano. La identidad digital, lejos de ser una simple representación de nuestras vidas en línea, se ha convertido en un aspecto central de nuestra existencia moderna, influyendo en cómo nos percibimos a nosotros mismos y en cómo somos percibidos por los demás en un mundo virtual. La identidad digital se constituye como un fenómeno fascinante que fusiona lo tangible con lo intangible, lo real con lo virtual.

Eres lo que publicas, construye tu identidad digital con cuidado.

Características de la identidad digital

La identidad digital se refiere a la representación de una persona en el mundo en línea, y está caracterizada por varios aspectos.



MATERIA CULTURA DIGITAL I

INFORMACIÓN SOBRE IDENTIDAD Y CREDENCIAL / LECTURA NO. 2

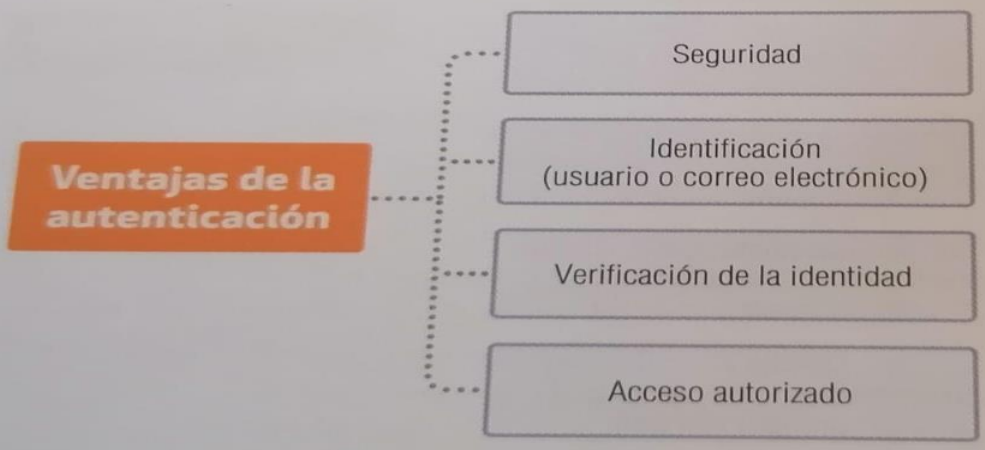
La identidad digital es una construcción compleja, pero, sobre todo, dinámica y subjetiva que se forma a través de la interacción en línea y puede tener repercusiones significativas en la vida real de una persona si no se tiene cuidado con la información que se comparte.

Algunos tips para proteger tu identidad digital

Contraseñas fuertes y únicas.
Autenticación de dos factores (A2F).
Revisa y ajusta regularmente las configuraciones de privacidad en tus cuentas en redes sociales y otras plataformas.
Limita la información personal que compartes públicamente.
Vigilancia de la información que compartes.
Evita publicar información sensible.
Actualizaciones de *software* y antivirus.
Mantén tu sistema operativo, navegadores y programas antivirus actualizados para protegerte contra posibles vulnerabilidades de seguridad.
Revise y ajusta los permisos de las aplicaciones regularmente para limitar el acceso a información innecesaria.
Concientización sobre *phishing*.
Sé cauteloso al hacer clic en enlaces o abrir correos electrónicos de fuentes desconocidas.
Utiliza conexiones seguras (**HTTPS**) al navegar por sitios web.
Realiza respaldo de datos importantes.
Mantente informado sobre las últimas amenazas y prácticas de seguridad.
Cierra sesión de tus cuentas cuando no las estés utilizando, especialmente en dispositivos compartidos.

Autenticación

La autenticación se refiere al proceso de verificación de la identidad de un usuario en un dispositivo o sistema para garantizar que la persona que intenta acceder a un recurso o servicio es quien dice ser. Este proceso es esencial en la actualidad, debido al creciente impacto de las TIC que utilizamos para realizar actividades cotidianas, por eso es importante proteger la seguridad de la información y prevenir accesos no autorizados. Algunas ventajas de implementar métodos de autenticación son:



Algunos métodos de autenticación

- Contraseñas
- Autenticación de dos factores (A2F) dos formas diferentes de autenticación
- Accesos biométricos (huella digital, reconocimiento facial, voz)
- Tarjetas inteligentes (Smart Cards)
- Certificados digitales
- Autenticación por SMS
- Token de seguridad

Algunos de ellos son comunes y fáciles de implementar, pero pueden ser vulnerables si son débiles o se comparten.

Impacto en la sociedad

La identidad digital impacta en la sociedad esencialmente en dos dimensiones.

1. Protege la privacidad, es decir, evita el mal uso de datos personales y posibles delitos como el robo de identidad, esto ayuda a construir una sociedad digital más confiable y segura.
2. Ayuda a la reputación en línea, la forma en cómo las otras personas nos perciben a través de internet, las oportunidades laborales y el fomento de un entorno en línea respetuoso.

Estos aspectos no sólo benefician individualmente, sino que también contribuyen a la construcción de una sociedad en línea más saludable, donde la confianza, el respeto y la ética digital son valores fundamentales determinando un impacto en la **autoimagen**, que puede ser una herramienta para expresar la autenticidad al conectar con otros de manera significativa.

Adaptación según contexto y sus recursos disponibles

Sabemos que en la actualidad nuestra presencia ***online*** define quiénes somos, navegar en este espacio digital requiere una visión profunda y una capacidad de adaptación al cambio, por lo que es fundamental conocer el entorno en el que operamos. Esto implica no sólo familiarizarse con las plataformas sociales y herramientas disponibles, sino también comprender las tendencias emergentes y las expectativas de la audiencia. La identidad digital se encuentra en constante innovación y se adapta al contexto y a los recursos disponibles. Por ejemplo, un ciudadano puede utilizar plataformas de educación en línea para mejorar sus habilidades, adaptándose al contexto laboral actual. Al mismo tiempo, esta identidad digital refleja la capacidad de aprovechar los recursos disponibles en el entorno digital para el crecimiento personal y profesional, según sea el caso.

Un aspecto importante a de considerar, es utilizar los recursos disponibles de manera efectiva. Esto puede incluir desde habilidades técnicas hasta herramientas de administración de redes sociales y acceso a redes de apoyo. Por ejemplo, al lanzar un negocio en línea, pueden aprovecharse plataformas de comercio electrónico para establecer tu tienda y utilizar redes sociales como Instagram y Facebook para promocionar tus productos.

La creatividad también juega un papel fundamental en este proceso. En un mundo saturado de contenido, destacar y captar la atención requiere pensar de manera innovadora y encontrar formas únicas de comunicar tu mensaje. Esto podría significar utilizar formatos de contenido novedosos.

La adaptación en el ámbito digital según tu contexto es un proceso continuo de innovación. No tengas miedo de experimentar y aprender de tus errores. Lo importante es estar siempre atento a los cambios y tomar las medidas necesarias para proteger tu identidad digital y tener siempre en cuenta el conocimiento del entorno, el uso efectivo de los recursos, y la creatividad e innovación. Dominar este arte te permitirá construir una presencia en línea sólida que te llevará al éxito.

El concepto de contraseña se desarrolló para ayudar a los usuarios a controlar el acceso hacia algún recurso que no queremos compartir, principalmente información. Las contraseñas son la principal barrera que evita que un actor malintencionado pueda acceder a nuestras redes sociales, correos electrónicos u otros servicios como el comercio on-line.

Al tener una función tan crítica, los ciberdelincuentes intentarán obtenerlas por todos los medios. En abril del 2021 Facebook fue víctima de una filtración de 500 millones de usuarios, entre la información filtrada se podía encontrar las direcciones de correo electrónico, la fecha de nacimiento, el número de teléfono o la ubicación geográfica de la persona.

En 2014, Forbes fue víctima de un ataque por el ciber ejército sirio, se filtraron los datos de 1 millón de usuarios, y también se publicaron las contraseñas de las víctimas.

Hay números casos de ataques como estos y por ello es de vital importancia tomar una serie de precauciones a la hora de configurar nuestras contraseñas para reducir los riesgos, especialmente cuando se trata de servicios abiertos a Internet.

ACCIONES PARA PREVENIR EL ROBO DE CREDENCIALES

1. CONCIENTIZACIÓN

Cualquier solicitud que pida checar unas credenciales debería considerarse sospecha. Al igual que con muchos aspectos de la ciberseguridad, la educación es clave para mitigar los ataques.

Por ejemplo, ¿Todos los empleados saben cómo reconocer un correo electrónico de phishing? El equipo de TI o de seguridad no debería ser el único grupo dentro de una empresa que sepa cómo identificar actividades potencialmente maliciosas.

La capacidad de reconocer cuándo las credenciales podrían verse comprometidas puede ahorrar pérdidas financieras.

2. USO SEGURO DE CONTRASEÑAS

La reutilización de contraseña debe evitarse a toda costa. En efecto, una vez que un atacante tiene una contraseña, puede probarla muy rápidamente en otros dominios para comprometer aún más los sistemas.

De la misma manera, compartir las credenciales entre las partes duplica el riesgo. A menudo tratando de ahorrar tiempo y dinero compartiendo suscripciones internamente en una empresa termina exponiendo las credenciales internamente y aumenta las posibilidades de compromiso.

3. RED TEAMING O ATAQUE SORPRESA

Para esto se usa un grupo de especialistas con experiencia táctica para poner a prueba los protocolos de seguridad de la organización. La idea es identificar las debilidades antes que los hackers. Para ser efectivos, deben operar de manera relativamente independiente, probando una variedad de técnicas de ataque sin previo aviso a los empleados.

Este tipo de ataques "sorpresa", de forma rutinaria pero irregular, pueden ser más efectivos para exponer defectos y debilidades en su postura de seguridad.

En general, el red teaming es un método inmensamente valioso para fortalecer la postura de seguridad de su organización.

4. CONTRASEÑAS DE UN SOLO USO, AUTENTICACIÓN DE DOS FACTORES, AUTENTICACIÓN DE MÚLTIPLES FACTORES

Muchos sitios ahora están usando procesos de autenticación de dos factores, desde preguntas de seguridad hasta tarjetas de identificación física y mensajes enviados a dispositivos móviles.

Aún más seguros son los procesos de autenticación que utilizan más de dos factores: la autenticación multifactor (MFA). La ventaja de usar estos es que es menos probable que un atacante tenga acceso a más de un factor que la contraseña robada.